Upper bounds for quantum biased oracles with explicit bias rate(New Trends in Theory of Computation and Algorithm)

AUTHOR(S):

Suzuki, Tomoya; Yamashita, Shigeru; Nakanishi, Masaki; Watanabe, Katsumasa

CITATION:

Suzuki, Tomoya ...[et al]. Upper bounds for quantum biased oracles with explicit bias rate(New Trends in Theory of Computation and Algorithm). 数理解析研究所講究録 2006, 1489: 135-141

ISSUE DATE:

2006-05

URL:

http://hdl.handle.net/2433/58217

数理解析研究所講究録
1489 巻 2006 年 135-141

Upper bounds for quantum biased oracles with explicit bias rate

鈴木 智哉 (Tomoya Suzuki), 山下 茂 (Shigeru Yamashita),
中西 正樹 (Masaki Nakanishi), 渡邊 勝正 (Katsumasa Watanabe)

奈良先端科学技術大学院大学 情報科学研究科
Graduate School of Information Science, Nara Institute of Science and Technology

Abstract — We investigate the query complexity of quantum biased oracles. Suppose that the biased oracles answer queries correctly with probability at least $1/2 + \varepsilon$. Given such an oracle, we present an algorithm to simulate a single query to an oracle that answers queries correctly with probability at least 2/3, using $O(1/\varepsilon)$ queries to the given oracle. For searching problems, combining the algorithm with a known result, we can obtain an optimal algorithm. The simulating algorithm works effectively when we know the value of ε. We also consider the situation where no knowledge about ε is given.

1 Introduction

In the quantum computing, *query complexity* is often used as a measure of the performance of algorithms. It is the number of calls of a black-box (often called *oracle*) computing a certain function f during running an algorithm. A *perfect* oracle receives x and returns $f(x)$ with certainty. On the other hand, a *biased* oracle, which we deal with in this paper, receives x and returns $f(x)$ with probability at least $1/2 + \varepsilon$. Since the algorithm depends on the oracle's outputs, the erroneous outputs from the biased oracle may need to be corrected to perform the algorithm properly. In general, the query complexity of biased oracles may increase compared to that of perfect oracles because of overheads for error-correction.

Majority voting is well-known as one of methods for error-correction. By using multiple queries to a given biased oracle and majority voting, we can increase the probability that the oracle answers each query correctly. It is known that $O(1/\varepsilon^2)$ queries are sufficient to increase the correct probability from $1/2 + \varepsilon$ to 2/3, and $O(\log T)$ queries are sufficient from 2/3 to $1 - 1/T$. Now, suppose that an algorithm uses T queries to a perfect oracle. In the algorithm, each query to the perfect oracle is simulated by $O\left(\frac{\log T}{\varepsilon^2}\right)$ queries to the corresponding biased oracle: As mentioned above, by $O\left(\frac{\log T}{\varepsilon^2}\right)$ queries and majority voting, we can increase the correct probability from $1/2 + \varepsilon$ to $1 - 1/T$ for each query, and if the correct probability of each query reaches $1 - 1/T$, the error probability piled up by T queries is upper-bounded by some constant. Thus it is known that $O\left(\frac{T \log T}{\varepsilon^2}\right)$ queries to a biased oracle are sufficient to perform any algorithms. It is optimal in some classical cases. On the other hand, in the quantum setting, a lower bound $\Omega(T/\varepsilon)$ by Iwama et al. [8] is only known, therefore the algorithms by the simple majority may not be optimal.

For some specific problems, $O(T/\varepsilon^2)$ quantum algorithms are known, which is efficient by a factor of $\log T$. For example, Høyer et al. presented a robust quantum search algorithm with $O(T/\varepsilon^2)$ queries in [7], and Buhrman et al. also showed $O(T/\varepsilon^2)$ algorithm for computing some functions such as parity with quantum biased oracles [4]. Moreover, Iwama et al. showed $O(T/\varepsilon)$ algorithms in a restricted setting or when $T \in O(1)$ in [8]. However, in the general biased setting, no quantum algorithm matching the corresponding lower bound has been presented.

Our contribution. We present an algorithm to simulate a single query to an oracle that answers each query correctly with probability at least 2/3, using $O(1/\varepsilon)$ queries to the given oracle that answers each query correctly with probability at least $1/2 + \varepsilon$. It implies that $O(1/\varepsilon^2)$ factors by majority voting can be replaced with new $O(1/\varepsilon)$ factors for any algorithms, since the simulating algorithm is independent of problems. Incorporating the robust quantum search algorithm by Høyer et al. [7], we can obtain an optimal algorithm to solve searching problems in an N-element space with $\Theta(\sqrt{N}/\varepsilon)$ queries to a biased oracle. The simulating algorithm does not work

effectively unless the value of ε is given. We also present a non-trivial algorithm to cope with a situation in which we have no prior knowledge about ε.

2 Preliminaries

In this section, we introduce the quantum computing and the query complexity. We also define quantum biased oracles.

2.1 Quantum state and evolution

A state of *n-qubit* quantum register $|\psi\rangle$ is a superposition of 2^n classical strings with length n, i.e., $|\psi\rangle = \sum_x \alpha_x |x\rangle$ where $x \in \{0,1\}^n$ and the *amplitudes* α_x are complex numbers consistent with the normalization condition: $\sum_x |\alpha_x|^2 = 1$. If we *measure* the state $|\psi\rangle$ with respect to the standard basis, we observe $|x\rangle$ with probability $|\alpha_x|^2$ and after the measurement the state $|\psi\rangle$ collapses into $|x\rangle$.

Without measurements, a quantum system can evolve satisfying the normalization condition. These evolutions are represented by unitary transformations. In this paper, unitary transformations controlled by other registers are often used. For example, one of them acts as some unitary transformation if the control qubit is $|1\rangle$, otherwise it acts as identity. The following operator Λ_M is also one of their applications.

Definition 1 *For any integer $M \geq 1$ and any unitary operator $\mathbf{U}$, the operator $\Lambda_M(\mathbf{U})$ is defined by*

$$|j\rangle|y\rangle \longmapsto \begin{cases} |j\rangle\mathbf{U}^j|y\rangle & (0 \leq j < M) \\ |j\rangle\mathbf{U}^M|y\rangle & (j \geq M). \end{cases}$$

Λ_M is controlled by the first register $|j\rangle$ in this case. $\Lambda_M(\mathbf{U})$ uses $\mathbf{U}$ for M times.

It is also known that quantum transformations can compute all classical functions. Let g be any classically computable function with m input and k output bits. Then, there exists a unitary transformation $\mathbf{U}_g$ corresponding to the computation of g: for any $x \in \{0,1\}^m$ and $y \in \{0,1\}^k$, $\mathbf{U}_g$ maps $|x\rangle|y\rangle$ to $|x\rangle|y \oplus g(x)\rangle$, where $\oplus$ denotes the bitwise exclusive-OR.

2.2 Query complexity

In this paper, we are interested in the query complexity, which is discussed in the following model. Suppose we want to compute some function $\mathcal{F}$ with an N-bit input and we can access each bit only through a given oracle O. The query complexity is the number of queries to the oracle. A quantum algorithm with T queries is a sequence of unitary transformations: $U_0 \to O_1 \to U_1 \to \ldots \to O_T \to U_T$, where O_i denotes the unitary transformation corresponding to the i-th query to the oracle O, and U_i denotes an arbitrary unitary transformation independent of the oracle. Our natural goal is to find an algorithm to compute $\mathcal{F}$ with sufficiently large probability and with the smallest number of oracle calls.

The most natural quantum oracles are quantum perfect oracles O_f that map $|x\rangle|0^{m-1}\rangle|0\rangle$ to $|x\rangle|0^{m-1}\rangle|f(x)\rangle$ for any $x \in [N]$. Here, $|0^{m-1}\rangle$ is a work register that is always cleared before and after querying oracles. On the other hand, quantum biased oracles, which we deal with in this paper, are defined as follows.

Definition 2 *A quantum oracle of a Boolean function f with bias ε is a unitary transformation O_f^ε or its inverse $O_f^{\varepsilon\dagger}$ such that*

$$O_f^\varepsilon|x\rangle|0^{m-1}\rangle|0\rangle = |x\rangle(\alpha_x|w_x\rangle|f(x)\rangle + \beta_x|w'_x\rangle|\overline{f(x)}\rangle),$$

where $|\alpha_x|^2 = 1/2 + \varepsilon_x \geq 1/2 + \varepsilon$ for any $x \in [N]$. Let also $\varepsilon_{min} = \min_x \varepsilon_x$.

Note that $0 < \varepsilon \leq \varepsilon_{min} \leq \varepsilon_x \leq 1/2$ for any x. In practice, ε is usually given in some way and ε_{min} or ε_x may be unknown. Unless otherwise stated, we discuss the query complexity with a given biased oracle O_f^ε in the rest of the paper.

3 Known results

3.1 Amplitude amplification

Brassard et al. showed amplitude amplification in [3], which is very useful to design quantum algorithms as follows. Suppose that we have a quantum algorithm $\mathcal{A}$ with success probability p. If there exists a Boolean function χ that can distinguish between success and fail (often called *good* and *bad* state), we can increase the success probability close to 1 by using $\mathcal{A}$ and χ for $O(1/\sqrt{p})$ times.

In the amplitude amplification, a unitary operator $\mathbf{Q} = -\mathcal{A}\mathbf{S}_0\mathcal{A}^{-1}\mathbf{S}_\chi$ is used. Here, $\mathbf{S}_0$ denotes an operator to flip the sign of amplitude of the state $|\mathbf{0}\rangle$, and $\mathbf{S}_\chi$ denotes an

operator to flip the signs of amplitudes of all the good states. Applying $\mathbf{Q}$ to the state $\mathcal{A}|0\rangle$ for j times, we have

$$\mathbf{Q}^j\mathcal{A}|0\rangle = \frac{1}{\sqrt{p}}\sin((2j+1)\theta_p)|\Psi_1\rangle + \frac{1}{\sqrt{1-p}}\cos((2j+1)\theta_p)|\Psi_0\rangle, \quad (1)$$

where $|\Psi_1\rangle$ has all the good states and $\langle\Psi_1|\Psi_1\rangle = p = \sin^2(\theta_p)$ and $|\Psi_1\rangle$ is orthogonal to $|\Psi_0\rangle$. After applying $\mathbf{Q}$ for about $\pi/4\theta_p \in O(1/\sqrt{p})$ times, we can measure a good solution with probability close to 1. Note that we need to know the value of p to do so. See [3] for more details.

Even if the success probability of $\mathcal{A}$, i.e., p is not given, we can have a good estimation of p as mentioned in Section 3.2. The next lemma in [8] states that the amplitude amplification works effectively when we know about the initial success probability p with some degree of precision.

Lemma 1 *Let $\mathcal{A}$ be any quantum algorithm that uses no measurements, and $\chi : \mathbf{Z} \to \{0,1\}$ be any Boolean function, and k be any integer at least 2. If $\tilde{\theta}_p$ is given such that $|\theta_p - \tilde{\theta}_p| \le \frac{\theta_p}{k(\pi+1)}$, where $p = \sin^2(\theta_p)$ is the initial success probability of $\mathcal{A}$ (i.e., the probability of outputting z such that $\chi(z) = 1$), and $0 \le \theta_p \le \pi/2$, then there exists a quantum algorithm that finds a good solution with probability at least $(1 - \frac{1}{k^2})$ using a number of applications of $\mathcal{A}$ and $\mathcal{A}^{-1}$ that is in $O(\frac{1}{\sqrt{p}})$.*

Proof Sketch. In [8], the algorithm by de-randomization idea is presented, which replaces the given algorithm $\mathcal{A}$ with a new algorithm $\mathcal{A}'$ with success probability p' slightly smaller than p. The algorithm adjusts the success probability p' and the number of applications of $\mathcal{A}'$ and χ (in precise, χ') suitably, to boost the success probability to almost equal to 1. It can be done as follows. At first, we compute the following four values: $m^* = \lceil \frac{1}{2}(\frac{\pi}{2\theta_p} - 1)\rceil$, $\theta_p^* = \frac{\pi}{4m^*+2}$, $p^* = \sin^2(\theta_p^*)$, and $\tilde{p} = \sin^2(\tilde{\theta}_p)$. m^* is used as the number of the applications of $\mathcal{A}'$ and χ'. The other values are used in making the new algorithm $\mathcal{A}'$: We rotate the last initialized qubit $|0\rangle$ into $\sqrt{\frac{p^*}{\tilde{p}}}|0\rangle + \sqrt{1-\frac{p^*}{\tilde{p}}}|1\rangle$ and regard the good state that has $|0\rangle$ in the last qubit as a new good state. This means that we have a new algorithm $\mathcal{A}'$ with success probability $p' = p\frac{p^*}{\tilde{p}} = \sin^2(\theta_{p'})$. After applying $\mathbf{Q}' = -\mathcal{A}'\mathbf{S}_0'\mathcal{A}'^{-1}\mathbf{S}_\chi$ to the state $\mathcal{A}'|0\rangle$ for m^* times, we have a good state $\frac{1}{\sqrt{p'}}\sin((2m^*+1)\theta_{p'})|\Psi_1'\rangle$ like Equation (1), and $\sin((2m^*+1)\theta_{p'}) \ge \sqrt{1-\frac{1}{k^2}}$ can be shown in this case.

3.2 Amplitude estimation

Brassard et al. also showed amplitude estimation in [3]. We rewrite it in terms of phase estimation for our convenience.

Theorem 2 *Let $\mathcal{A}, \chi$, and θ_p be as in Lemma 1. There exists a quantum algorithm Est_Phase($\mathcal{A}, \chi, M$) that outputs $\tilde{\theta}_p$ such that $|\theta_p - \tilde{\theta}_p| \le \frac{\pi}{M}$, with probability at least $\frac{8}{\pi^2}$. It uses exactly M invocations of $\mathcal{A}$ and χ, respectively. If $\theta_p = 0$ then $\tilde{\theta}_p = 0$ with certainty, and if $\theta_p = \frac{\pi}{2}$ and M is even, then $\tilde{\theta}_p = \frac{\pi}{2}$ with certainty.*

3.3 Robust quantum search

Grover showed a quantum search algorithm that finds a solution in an N-element space [6]. It uses $O(\sqrt{N})$ queries to a perfect oracle O_f to check whether the i-th element is a solution or not. Høyer et al. showed a robust quantum search algorithm in [7]. It uses a biased oracle $O_f^{2/5}$ instead of a perfect oracle to access the elements, and it finds a solution by using $O(\sqrt{N})$ queries to the biased oracle, which has no overheads for error-correction as stated in the following theorem formally.

Theorem 3 *There exists a quantum algorithm that outputs x such that $f(x) = 1$, if any, with probability at least $2/3$ using $O(\sqrt{N})$ queries to the given oracle $O_f^{2/5}$.*

4 Upper bound with known ε

In this section, we present a quantum algorithm to simulate a single query to an oracle $O_f^{1/6}$ by $O(1/\varepsilon)$ queries to a given oracle O_f^ε with known ε. At the end of this section a quantum algorithm for searching problems with biased oracles is also presented and it can be seen that the algorithm is optimal.

Before presenting the simulating algorithm in Theorem 6, we show that we can replace the given oracle O_f^ε with a new oracle $\tilde{O}_f^\varepsilon$. The next lemma describes the oracle $\tilde{O}_f^\varepsilon$ and how to construct it from O_f^ε.

Lemma 4 *There exists a quantum oracle $\tilde{O}_f^\varepsilon$ that consists of one O_f^ε and one $O_f^{\varepsilon\dagger}$ such that for any $x \in [N]$*

$$\tilde{O}_f^\varepsilon|x,0^m,0\rangle = (-1)^{f(x)}2\varepsilon_x|x,0^m,0\rangle + |x,\psi_x\rangle, \quad (2)$$

where $|x,\psi_x\rangle$ is orthogonal to $|x,0^m,0\rangle$ and its norm is $\sqrt{1-4{\varepsilon_x}^2}$.

Proof We can show the construction of $\tilde{O}_f^{\varepsilon}$ in a similar way in Lemma 1 in [8]. □

Now, we describe our approach to simulate an oracle $O_f^{1/6}$ by the given oracle O_f^{ε}. According to [8], if the query register $|x\rangle$ is not in a superposition, phase flip oracles can be simulated with sufficiently large probability: by using amplitude estimation through $\tilde{O}_f^{\varepsilon}$, we can estimate the value of ε_x, then by using the estimated value and applying amplitude amplification to the state in Equation (2), we can obtain the state $(-1)^{f(x)}|x,0^m,0\rangle$ with high probability. In Theorem 6, we essentially simulate the phase flip oracle by using the above algorithm in a superposition of $|x\rangle$. Note that we convert the phase flip oracle into the bit flip version in the theorem.

We will present the simulating algorithm after the following lemma, which shows that amplitude estimation can work in quantum parallelism. *Est_Phase* in Theorem 2 is straightforwardly extended to *Par_Est_Phase* in Lemma 5. We omit the proof of Lemma 5.

Lemma 5 *Let $\chi : \mathbf{Z} \to \{0,1\}$ be any Boolean function, and let O be any quantum oracle that uses no measurements such that*

$$O|x\rangle|\mathbf{0}\rangle = |x\rangle O_x|\mathbf{0}\rangle = |x\rangle|\Psi_x\rangle = |x\rangle(|\Psi_x^1\rangle + |\Psi_x^0\rangle),$$

where a state $|\Psi_x\rangle$ is divided into a good state $|\Psi_x^1\rangle$ and a bad state $|\Psi_x^0\rangle$ by χ. Let $\sin^2(\theta_x) = \langle\Psi_x^1|\Psi_x^1\rangle$ be the success probability of $O_x|\mathbf{0}\rangle$ where $0 \le \theta_x \le \pi/2$. There exists a quantum algorithm Par_Est_Phase(O,χ,M) that changes states as follows:

$$|x\rangle|\mathbf{0}\rangle|\mathbf{0}\rangle \longmapsto |x\rangle \otimes \sum_{j=0}^{M-1} \delta_{x,j}|v_{x,j}\rangle|\tilde{\theta}_{x,j}\rangle,$$

where $\sum_{j:|\theta_x-\tilde{\theta}_{x,j}|\le\frac{\pi}{M}} |\delta_{x,j}|^2 \ge \frac{8}{\pi^2}$ for any x, and $|v_{x,i}\rangle$ and $|v_{x,j}\rangle$ are mutually orthonormal vectors for any i, j. It uses O and its inverse for $O(M)$ times.

Now, we show a whole algorithm to construct an oracle $O_f^{1/6}$ from O_f^{ε} by $O(1/\varepsilon)$ queries with known ε.

Theorem 6 *There exists a quantum algorithm that simulates a single query to an oracle $O_f^{1/6}$ by using $O(1/\varepsilon)$ queries to O_f^{ε} if we know ε.*

Proof

We will show a quantum algorithm that changes states as follows:

$$|x\rangle|\mathbf{0}\rangle|0\rangle \longmapsto |x\rangle(\alpha_x|w_x\rangle|f(x)\rangle + \beta_x|w_x'\rangle|\overline{f(x)}\rangle),$$

where $|\alpha_x|^2 \ge 2/3$ for any x, using $O(1/\varepsilon)$ queries to O_f^{ε}. The algorithm performs amplitude amplification following amplitude estimation in a superposition of $|x\rangle$.

At first, we use amplitude estimation in parallel to estimate ε_x or to know how many times the following amplitude amplification procedures should be repeated. Let $\sin\theta = 2\varepsilon$ and $\sin\theta_x = 2\varepsilon_x$ such that $0 < \theta, \theta_x \le \pi/2$. Note that $\Theta(\theta) = \Theta(\varepsilon)$ since $\sin\theta \le \theta \le \frac{\pi}{2}\sin\theta$ when $0 \le \theta \le \pi/2$. Let also $M_1 = \left\lceil \frac{3\pi(\pi+1)}{\theta} \right\rceil$ and χ be a Boolean function that divides a state in Equation (2) into a good state $(-1)^{f(x)}2\varepsilon_x|0^{m+1}\rangle$ and a bad state $|\psi_x\rangle$. The function χ checks only whether the state is $|0^{m+1}\rangle$ or not; therefore, it is implemented easily. By Lemma 5, *Par_Est_Phase*$(\tilde{O}_f^{\varepsilon},\chi,M_1)$ maps

$$|x\rangle|\mathbf{0}\rangle|\mathbf{0}\rangle|\mathbf{0}\rangle \longmapsto |x\rangle \otimes \sum_{j=0}^{M-1} \delta_{x,j}|v_{x,j}\rangle|\tilde{\theta}_{x,j}\rangle|\mathbf{0}\rangle,$$

where $\sum_{j:|\theta_x-\tilde{\theta}_{x,j}|\le\frac{\theta}{3(\pi+1)}} |\delta_{x,j}|^2 \ge \frac{8}{\pi^2}$ for any x, and $|v_{x,i}\rangle$ and $|v_{x,j}\rangle$ are mutually orthonormal vectors for any i, j. This state has the good estimations of θ_x in the third register with high probability. The fourth register $|\mathbf{0}\rangle$ remains large enough to perform the following steps.

The remaining steps basically perform amplitude amplification by using the estimated values $\tilde{\theta}_{x,j}$, which can realize a phase flip oracle. Note that in the following steps a pair of Hadmard transformations are used to convert the phase flip oracle into our targeted oracle.

Based on the de-randomization idea as in [8], we calculate $m_{x,j}^* = \left\lceil \frac{1}{2}\left(\frac{\pi}{2\tilde{\theta}_{x,j}} - 1\right)\right\rceil$, $\theta_{x,j}^* = \frac{\pi}{4m_{x,j}^*+2}$, $p_{x,j}^* = \sin^2(\theta_{x,j}^*)$ and $\tilde{p}_{x,j} = \sin^2(\tilde{\theta}_{x,j})$ in the superposition, and apply an Hadmard transformation to the last qubit. Thus we have

$$|x\rangle\Big(\sum_{j=0}^{M-1} \delta_{x,j}|v_{x,j}\rangle|\tilde{\theta}_{x,j}\rangle|m_{x,j}^*\rangle|\theta_{x,j}^*\rangle|p_{x,j}^*\rangle|\tilde{p}_{x,j}\rangle \otimes |0^{m+1}\rangle|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\Big).$$

Let $\mathbf{R} : |0\rangle \to \sqrt{\frac{p_{x,j}^*}{\tilde{p}_{x,j}}}|0\rangle + \sqrt{1-\frac{p_{x,j}^*}{\tilde{p}_{x,j}}}|1\rangle$ be a rotation and let $\mathbf{O} = \tilde{O}_f^{\varepsilon} \otimes \mathbf{R}$ be a new oracle. We apply $\mathbf{O}$ followed by

$\Lambda_{M_2}(\mathbf{Q})$, where $M_2 = \left\lceil \frac{1}{2}\left(\frac{3\pi(\pi+1)}{2(3\pi+2)\theta} + 1\right)\right\rceil$ and $\mathbf{Q} = -\mathbf{O}(\mathbf{I}\otimes \mathbf{S}_0)\mathbf{O}^{-1}(\mathbf{I}\otimes \mathbf{S}_\chi)$; $\mathbf{S}_0$ and $\mathbf{S}_\chi$ are defined appropriately. Λ_{M_2} is controlled by the register $|m^*_{x,j}\rangle$, and $\mathbf{Q}$ is applied to the registers $|x\rangle$ and $|0^{m+1}\rangle|0\rangle$ if the last qubit is $|1\rangle$. Let $\mathbf{O}_x$ denote the unitary operator such that $\mathbf{O}|x\rangle|0^{m+1}\rangle|0\rangle = |x\rangle\mathbf{O}_x|0^{m+1}\rangle|0\rangle$. Then we have the state (From here, we write only the last three registers.)

$$\sum_{j=0}^{M-1} \frac{\delta_{x,j}}{\sqrt{2}}\left(|0^{m+1}\rangle|0\rangle|0\rangle + \mathbf{Q}_x^{m_{x,j}}\mathbf{O}_x\left(|0^{m+1}\rangle|0\rangle\right)|1\rangle\right), \quad (3)$$

where $\mathbf{Q}_x = -\mathbf{O}_x\mathbf{S}_0\mathbf{O}_x^{-1}\mathbf{S}_\chi$ and $m_{x,j} = \min(m^*_{x,j}, M_2)$ for any x, j. We will show that the phase flip oracle is simulated if the third register $|\tilde{\theta}_{x,j}\rangle$ has the good estimation of θ_x and the last register has $|1\rangle$. Equation (3) can be rewritten as

$$\sum_{j=0}^{M-1} \frac{\delta_{x,j}}{\sqrt{2}}\left(|0^{m+1},0\rangle|0\rangle + \left((-1)^{f(x)}\gamma_{x,j}|0^{m+1},0\rangle + |\varphi_{x,j}\rangle\right)|1\rangle\right),$$

where $|\varphi_{x,j}\rangle$ is orthogonal to $|0^{m+1},0\rangle$ and its norm is $\sqrt{1-\gamma_{x,j}^2}$. Suppose that the third register has $|\tilde{\theta}_{x,j}\rangle$ such that $|\theta_x - \tilde{\theta}_{x,j}| \le \frac{\theta_x}{3(\pi+1)}$. It can be seen that $m_{x,j} \le M_2$ if $|\theta_x - \tilde{\theta}_{x,j}| \le \frac{\theta_x}{3(\pi+1)}$. Therefore, $\mathbf{Q}_x$ is applied for $m^*_{x,j}$ times, i.e., the number specified by the fourth register. Like the analysis of Lemma 2 in [8], it is shown that $\gamma_{x,j} \ge \sqrt{1-\frac{1}{9}}$.

Finally, applying an Hadmard transformation to the last qubit again, we have the state

$$\sum_{j=0}^{M-1} \frac{\delta_{x,j}}{2}\Big((1+(-1)^{f(x)}\gamma_{x,j})|0^{m+2}\rangle|0\rangle + (1-(-1)^{f(x)}\gamma_{x,j})|0^{m+2}\rangle|1\rangle + |\varphi_{x,j}\rangle(|0\rangle - |1\rangle)\Big).$$

If we measure the last qubit, we have $|f(x)\rangle$ with probability

$$\sum_{j=0}^{M-1}\left(\left|\frac{\delta_{x,j}(1+\gamma_{x,j})}{2}\right|^2 + \left|\frac{\delta_{x,j}\sqrt{1-\gamma_{x,j}^2}}{2}\right|^2\right) \ge \frac{1}{2}\sum_{j:|\theta_x-\tilde{\theta}_{x,j}|\le\frac{\theta}{3(\pi+1)}} |\delta_{x,j}|^2\left(1+\gamma_{x,j}\right) \ge \frac{2}{3}.$$

Thus, the final quantum state can be rewritten as $|x\rangle(\alpha_x|w_x\rangle|f(x)\rangle + \beta_x|w'_x\rangle|\overline{f(x)}\rangle)$, where $|\alpha_x|^2 \ge 2/3$ for any x.

The query complexity of this algorithm is the cost of amplitude estimation M_1 and amplitude amplification M_2, thus a total number of queries is $O(\frac{1}{\theta}) = O(\frac{1}{\varepsilon})$. Therefore, we can simulate a single query to $O_f^{1/6}$ using $O(\frac{1}{\varepsilon})$ queries to O_f^{ε}. □

From Theorem 3 and Theorem 6 we can derive the following corollary directly.

Corollary 7 *There exists a quantum algorithm which outputs x such that $f(x) = 1$, if any, with probability at least $2/3$ using $O(\frac{\sqrt{N}}{\varepsilon})$ queries to a given oracle O_f^{ε} if we know ε. Moreover, if we know ε_{min}, the algorithm uses $\Theta\left(\frac{\sqrt{N}}{\varepsilon_{min}}\right)$ queries.*

For searching problems, lower bound $\Omega\left(\frac{\sqrt{N}}{\varepsilon_{min}}\right)$ is proved by Theorem 6 in [8] based on Ambainis' method [2]. Thus, we can see the above matching bound when $\varepsilon = \varepsilon_{min}$.

5 Upper bound without knowing ε

In Section 4, we described algorithms by using a given oracle O_f^{ε} when we know ε. In this section, we assume that there is no prior knowledge of ε.

Our overall approach is to estimate ε (in precise ε_{min}) with appropriate accuracy in advance, which then can be used in the simulating algorithm in Theorem 6. In the following, we first describe an overview of our strategy to estimate ε_{min} rather informally, followed by rigorous and detailed descriptions.

First, let us consider estimating ε_x in the same way as in Theorem 6 in quantum parallelism. Then, let M^* denote the number of required oracle calls to achieve a *good* estimation of ε_x for any x. (Here, *good* means accurate enough to perform effective amplitude amplification in Theorem 6.) Note that $M^* \in \Omega(1/\varepsilon_{min})$, and if we know the value of ε, we can set $\Theta(1/\varepsilon)$ as M^*. However, now ε is unknown, we estimate M^* as follows. First we will construct an algorithm, $\mathcal{A}_{enough}$, which receives an input M and decides whether M is the number of oracle calls to obtain a good estimation of ε_x. More precisely, $\mathcal{A}_{enough}$ uses $O(M)$ queries and returns 0 if the input M is large enough to estimate ε_x, otherwise it returns 1 with a more than constant probability, say, 9/10. Then, by using $\mathcal{A}_{enough}$ in a superposition of $|x\rangle$ as in Lemma 8, we can obtain the state $\sum_x |x\rangle\otimes(\alpha_x|u_x\rangle|1\rangle + \beta_x|u'_x\rangle|0\rangle)$. When M is small, the condition $\exists x; |\alpha_x|^2 \ge 9/10$ holds, which means

there exists x such that the estimation of ε_x may be bad. On the other hand, when M is sufficiently large, the condition $\forall x; |\alpha_x|^2 \leq 1/10$ holds, which means the estimation is good for any x. Our remaining essential task, then, is to know an input value of M at the verge of the above two cases. Note that the value is $\Theta(1/\varepsilon_{min})$, which can be used as M^*.

Next, we consider an algorithm, A_{check}, which can distinguish the above two cases with $O(T)$ oracle queries with a constant probability. Then, M^* can be estimated by $O(TM^* \log\log M^*)$ queries by the following search technique and majority voting: We can find M^* by trying $\mathcal{A}_{check}$ along with exponentially increasing the input value M until $\mathcal{A}_{check}$ succeeds. Note that a $\log\log M^*$ factor is needed to boost the success probability of $\mathcal{A}_{check}$ to close to 1. It should be noted that we cannot use robust quantum search algorithm [7] as $\mathcal{A}_{check}$, since there may exist x such that $|\alpha_x|^2 \approx 1/2$, which cannot be dealt with by their algorithm. Instead, in Lemma 9, we will describe the algorithm $\mathcal{A}_{check}$, which can distinguish the above two cases by using amplitude estimation querying for $O(\sqrt{N}\log N)$ times. Then, the whole algorithm requires $O(TM^* \log\log M^*) = O\left(\frac{\sqrt{N}\log N}{\varepsilon_{min}} \log\log \frac{1}{\varepsilon_{min}}\right)$ queries. In Lemma 8, we present an algorithm *Par_Est_Zero* that acts as $\mathcal{A}_{enough}$ in a superposition of $|x\rangle$, and in Lemma 9, we describe the algorithm *Chk_Amp_Dn* as $\mathcal{A}_{check}$. Finally, the whole algorithm to estimate M^* is presented in Theorem 10.

Lemma 8 *Let O be any quantum algorithm that uses no measurements such that $O|x\rangle|\mathbf{0}\rangle = |x\rangle|\Psi_x\rangle = |x\rangle(|\Psi_x^1\rangle + |\Psi_x^0\rangle)$. Let $\chi : \mathbf{Z} \to \{0,1\}$ be a Boolean function that divides a state $|\Psi_x\rangle$ into a good state $|\Psi_x^1\rangle$ and a bad state $|\Psi_x^0\rangle$ such that $\sin^2(\theta_x) = \langle\Psi_x^1|\Psi_x^1\rangle$ for any x $(0 < \theta_x \leq \pi/2)$. There exists a quantum algorithm Par_Est_Zero(O,χ,M) that changes states as follows:*

$$|x\rangle|\mathbf{0}\rangle|0\rangle \to |x\rangle \otimes (\alpha_x|u_x\rangle|1\rangle + \beta_x|u_x'\rangle|0\rangle),$$

where $|\alpha_x|^2 = \dfrac{\sin^2(M\theta_x)}{M^2\sin^2(\theta_x)}$ for any x. It uses O and its inverse for $O(M)$ times.

The algorithm *Par_Est_Zero* can be implemented like *Par_Est_Phase* in Lemma 5. We omit details.

Lemma 9 *Let O be any quantum oracle such that $O|x\rangle|\mathbf{0}\rangle|0\rangle = |x\rangle(\alpha_x|w_x\rangle|1\rangle + \beta_x|u_x\rangle|0\rangle)$. There exists a quantum algorithm Chk_Amp_Dn(O) that outputs $b \in \{0,1\}$ such that*

$$b = \begin{cases} 1 & \text{if } \exists x; |\alpha_x|^2 \geq \frac{9}{10} \\ 0 & \text{if } \forall x; |\alpha_x|^2 \leq \frac{1}{10} \\ \text{don't care} & \text{otherwise,} \end{cases}$$

with probability at least $8/\pi^2$ using $O(\sqrt{N}\log N)$ queries to O.

Proof Sketch. Using $O(\log N)$ applications of O and majority voting, we have a new oracle O' such that

$$O'|x\rangle|\mathbf{0}\rangle|0\rangle = |x\rangle(\alpha_x'|w_x'\rangle|1\rangle + \beta_x'|u_x'\rangle|0\rangle),$$

where $|\alpha_x'|^2 \geq 1 - \frac{1}{16N}$ if $|\alpha_x|^2 \geq \frac{9}{10}$, and $|\alpha_x'|^2 \leq \frac{1}{16N}$ if $|\alpha_x|^2 \leq \frac{1}{10}$. *Est_Phase* can distinguish the two cases, i.e., $\exists x; |\alpha_x|^2 \geq \frac{9}{10}$ and $\forall x; |\alpha_x|^2 \leq \frac{1}{10}$ by $O(\sqrt{N})$ queries to O' with high probability.

Theorem 10 *Given a quantum biased oracle O_f^ε, there exists a quantum algorithm Est_Eps_Min(O_f^ε) that outputs $\tilde{\varepsilon}_{min}$ such that $\varepsilon_{min}/5\pi^2 \leq \tilde{\varepsilon}_{min} \leq \varepsilon_{min}$ with probability at least 2/3. The query complexity of the algorithm is expected to be $O\left(\frac{\sqrt{N}\log N}{\varepsilon_{min}} \log\log \frac{1}{\varepsilon_{min}}\right)$.*

Proof Let $\sin(\theta_x) = 2\varepsilon_x$ and $\sin(\theta_{min}) = 2\varepsilon_{min}$ such that $0 < \theta_x, \theta_{min} \leq \frac{\pi}{2}$. Let χ also be a Boolean function that divides the state in Equation (2) into a good state $(-1)^{f(x)}2\varepsilon_x|0^{m+1}\rangle$ and a bad state $|\psi_x\rangle$. Thus *Par_Est_Zero*$(\tilde{O}_f^\varepsilon, \chi, M)$ in Lemma 8 makes the state $|x\rangle \otimes (\alpha_x|u_x\rangle|1\rangle + \beta_x|u_x'\rangle|0\rangle)$ such that $|\alpha_x|^2 = \frac{\sin^2(M\theta_x)}{M^2\sin^2(\theta_x)}$. As stated below, if $M \in o(1/\theta_x)$, then $|\alpha_x|^2 \geq 9/10$. We can use *Chk_Amp_Dn* to check whether there exists x such that $|\alpha_x|^2 \geq 9/10$. Based on these facts, we present the whole algorithm *Est_Eps_Min*(O_f^ε).

Algorithm(*Est_Eps_Min*(O_f^ε) **)**

1. Start with $\ell = 0$.
2. Increase ℓ by 1.
3. Run *Chk_Amp_Dn*(*Par_Est_Zero*$(\tilde{O}_f^\varepsilon, \chi, 2^\ell)$) for $O(\log \ell)$ times and use majority voting. If "1" is output as the result of the majority voting, then return to Step 2.
4. Output $\tilde{\varepsilon}_{min} = \frac{1}{2}\sin\left(\frac{1}{5\cdot 2^\ell}\right)$.

Now, we will show that the algorithm almost keeps running until $\ell > \lfloor \log_2 \frac{1}{5\theta_{min}} \rfloor$. We assume $\ell \leq \lfloor \log_2 \frac{1}{5\theta_{min}} \rfloor$. Under this assumption, a proposition $\exists x; |\alpha_x|^2 \geq \frac{9}{10}$ holds since the equation $\varepsilon_{min} = \min_x \varepsilon_x$ guarantees that there exists some x such that $\theta_{min} = \theta_x$ and $|\alpha_x|^2 = \frac{\sin^2(2^\ell \theta_x)}{2^{2\ell}\sin^2(\theta_x)} \geq \cos^2(\frac{1}{5}) > \frac{9}{10}$ when $2^\ell \leq \frac{1}{5\theta_x}$. Therefore, a single *Chk_Amp_Dn* run returns "1" with probability at least $8/\pi^2$. By $O(\log \ell)$ repetitions and majority voting, the probability that we obtain "1" increases to at least $1 - \frac{1}{5\ell^2}$. Consequently, the overall probability that we return from Step 3 to Step 2 for any ℓ such that $\ell \leq \lfloor \log_2 \frac{1}{5\theta_{min}} \rfloor$ is at least $\prod_{\ell=1}^{\lfloor \log_2 \frac{1}{5\theta_{min}} \rfloor} \left(1 - \frac{1}{5\ell^2}\right) > \frac{2}{3}$. This inequality can be obtained by considering an infinite product expansion of $\sin(x)$, i.e., $\sin(x) = x\prod_{n=1}^{\infty}\left(1 - \frac{x^2}{n^2\pi^2}\right)$ at $x = \pi/\sqrt{5}$. Thus the algorithm keeps running until $\ell > \lfloor \log_2 \frac{1}{5\theta_{min}} \rfloor$, i.e., outputs $\tilde{\varepsilon}_{min}$ such that $\tilde{\varepsilon}_{min} = \frac{1}{2}\sin\left(\frac{1}{5\cdot 2^\ell}\right) \leq \frac{1}{2}\sin(\theta_{min}) = \varepsilon_{min}$, with probability at least $2/3$.

We can also show that the algorithm almost stops in $\ell < \lceil \log_2 \frac{2\pi}{\theta_{min}} \rceil$. Since $\frac{\sin^2(M\theta)}{M^2\sin^2(\theta)} \leq \frac{\pi^2}{(2M\theta)^2}$ when $0 \leq \theta \leq \frac{\pi}{2}$, $|\alpha_x|^2 = \frac{\sin^2(2^\ell\theta_x)}{2^{2\ell}\sin^2(\theta_x)} \leq \frac{1}{16}$ for any x if $2^\ell \geq \frac{2\pi}{\theta_{min}}$. Therefore, in Step 3, "0" is returned with probability at least $8/\pi^2$ when $\ell \geq \lceil \log_2 \frac{2\pi}{\theta_{min}} \rceil$. The algorithm, thus, outputs $\tilde{\varepsilon}_{min} = \frac{1}{2}\sin\left(\frac{1}{5\cdot 2^\ell}\right) \geq \frac{1}{2}\sin\left(\frac{\theta_{min}}{10\pi}\right) \geq \frac{\varepsilon_{min}}{5\pi^2}$ with probability at least $8/\pi^2$.

Let $\tilde{\ell}$ satisfy $\lfloor \log_2 \frac{1}{5\theta_{min}} \rfloor < \tilde{\ell} < \lceil \log_2 \frac{2\pi}{\theta_{min}} \rceil$. If the algorithm runs until $\ell = \tilde{\ell}$, its query complexity is

$$\sum_{\ell=1}^{\tilde{\ell}} O(2^\ell \sqrt{N}\log N \log \ell) = O(2^{\tilde{\ell}}\sqrt{N}\log N \log \tilde{\ell})$$
$$= O\left(\frac{\sqrt{N}\log N}{\varepsilon_{min}} \log\log \frac{1}{\varepsilon_{min}}\right),$$

since $2^{\tilde{\ell}} \in \Theta\left(\frac{1}{\theta_{min}}\right) = \Theta\left(\frac{1}{\varepsilon_{min}}\right)$. □

6 Conclusion

We have shown an algorithm to simulate a single query to an oracle $O_f^{1/6}$ by using $O(1/\varepsilon)$ queries to the given oracle O_f^{ε} when ε is known. Since this algorithm is independent of problems, overhead factors $O(1/\varepsilon^2)$ by majority can be replaced with new factors $O(1/\varepsilon)$ in general. As a result, we can obtain an optimal algorithm for searching problems in the quantum biased setting. We have also considered the situation in which no knowledge about the oracle's bias is given. Namely, we have presented a nontrivial algorithm to estimate ε_{min}.

Future works. When ε is not given, there remains a gap between the upper bound and the lower bound for searching problems. To match their bounds is a next important topic. The algorithm to estimate ε_{min} seems to have room for improvements.

It is also interesting to find other matching bounds for quantum biased oracles. An improvement for upper bounds is one approach to do so. For example, it is challenging to find algorithms using a biased oracle $O_f^{1/6}$ without $O(\log T)$ overhead factor. The other is an improvement for lower bounds. Since it is likely impossible to improve the general lower bound $\Omega(T/\varepsilon)$, we should consider lower bounds for specific problems.

References

[1] Mark Adcock and Richard Cleve. A quantum goldreich-levin theorem with cryptographic applications. In *STACS*, pages 323–334, 2002.

[2] Andris Ambainis. Quantum lower bounds by quantum arguments. *J. Comput. Syst. Sci.*, 64(4):750–767, 2002.

[3] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. In *Quantum Computation & Information*, volume 305 of *AMS Contemporary Mathematics Series Millenium Volume*, pages 53–74, 2002.

[4] Harry Buhrman, Ilan Newman, Hein Röhrig, and Ronald de Wolf. Robust polynomials and quantum algorithms. In *STACS*, pages 593–604, 2005.

[5] Uriel Feige, Prabhakar Raghavan, David Peleg, and Eli Upfal. Computing with noisy information. *SIAM J. Comput.*, 23(5):1001–1018, 1994.

[6] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *STOC*, pages 212–219, 1996.

[7] Peter Høyer, Michele Mosca, and Ronald de Wolf. Quantum search on bounded-error inputs. In *ICALP*, pages 291–299, 2003.

[8] Kazuo Iwama, Rudy Raymond, and Shigeru Yamashita. General bounds for quantum biased oracles. *IPSJ Journal*, 46(10):1234–1243, 2005.